KPMG Cyber Threat Intelligence Platform

Trigona- Emerging New Ransomware

Trigona ransomware, named after stingless bees & written in the Delphi programming language debuted in late October 2022. It has remained highly active, impacting nearly 17 organizations, including notable incidents in December 2022. The group is observed to have links to BlackCat using the latter's reputation & leak site for additional extortion pressure. Also, overlap of infrastructure including file names, IP addresses & payloads with Gang 8220 & similarities in ransom note format & encryption type with CryLock are spotted. Its impact spans sectors across manufacturing, finance, construction, agriculture & marketing in the U.S., France, Germany, Italy, Australia, New Zealand & India.

Initial attack vector includes phishing emails, brute-forcing poorly configured MS-SQL servers, exploiting ManageEngine vulnerability - CVE-2021-40539 & exposed RDP services. The attacker employs a UPX packed, password protected version of Mimikatz to dump, inject and manipulate credentials. Batch scripts perform various tasks, including copying malicious tools & exe files, clearing shadow copies, recycle bin event logs, & terminating services. Attackers ensures persistence by modifying Run registry key, creating privileged users, to perform network scanning, opening firewall ports, bypassing UAC & enabling sticky keys backdoor. A remote access tool called Splashtop is used for lateral movement, executing commands and maintaining access. Prior to exfiltration and encryption, drives & networks are enumerated. To cover their attacks, the malware deletes files by overwriting them with NULL and drops a ransom note in HTA format with a unique victim ID in JavaScript. It proceeds to encryption using RSA & AES in OFB mode.

Trigona ransomware, with its uncommon evasion techniques like password protected executables, highlights the need for proactive measures like software updates and data backups to ensure protection.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Trigona- Emerging New Ransomware

Indicators of Compromise: IP Addresses	
45.227.253[.]98	45.227.253[.]107
45.227.253[.]99	45.227.253[.]106
128.90.173[.]138	193.149.185[.]117

Indicators of Compromise: Domains
3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion

Indicators of Compromise: Hashes
f2a9c02d1ee21d476e727a107c626028
738178902799d2ba7814e8a4e548fd47
11ed19d5adba04a194ad98bb30f37f4f
d5b32ca6961a61af5920231046fe6399
fcfc94b1d9b3c02c3e178e25803f5e7b
ea4dd9dd50f47ea1e0aa1a2165f75227
9d01ef99b9f37f5b8d66b42a7696892c
c2bf1ff3cdf1f5e85fe59bfc1ac4cc99
924d4072a0976775a81a4cfe683cee5b
46b639d59fea86c21e5c4b05b3e29617
5db23a2c723cbceabec8d5e545302dc4
1a877b9f532a2cee135e5e4efede9131
eb9fdc083164c0cead39fecaad9aafb4
abc9b951946c6313cd6c0c8f27d72f07
e248e214c121845e69bbf266cc9e2853
b02301c3c8e078e2287c1fbca12f8a00
a031edc72ddea262780560405c0ea4ae
ae44e63b881e362cc6249f7dfdaa50ca
17576d27c0bcd5ab82a73f0b7d4a3e55
db9db1adf096eac42a0661731af4e901
d57507d21747f6d6da3ebf02a0854bc3
cd215489a03871eaac431180546f162e
845f96b54fecfa365c686625fecdf210
0a8ee230e5390b8855b1968daee6827e
1cece45e368656d322b68467ad1b8c02

KPMG

KPMG Cyber Threat Intelligence Platform

Trigona- Emerging New Ransomware

Indicators of Compromise: Hashes
530967fb3b7d9427552e4ac181a37b9a
2473044423d6e46f467cea92c18766bd
67dd0708a2dcbe6b7661fd5eb4593ea7
41bcf469661ab9609a0d181953c2f8ffb75bb483
c609ec0c1061fe3f04bc30e965a4d3d2450bd8d1
672c0f37540788ba3332f1093b7b6b7b8817e27a
4004732202121a62ea17058eb94b825cbf486ef5
00b00de2cdb999c59dfbf56cd95cf00249ddd018
61ab50c08abb92ed76755fbff726a93c43fa0619
134fe10e2c0858417141d4c95315d26216dd4330
b13744f6af6ba475cb0b5aa92c7ba197808827d6
910d65e5754c8ee976629ae05de62531b7412ec7
af5b85d2d856932c101723909a20a61a91976da7
bd58d5080ab10102c5431d80715b0a8df4c501f0
76c86e4f5f4c16a284c2ec2e2d6bb647a0ace672
356c09ec8b349e0ed2e58dc5fda1d8c68d643c3d
b2f3a868a1cae39657b32cb2b8514cb278a05585
19c8782165f56d4153658da5f88f9edd14ae2022
21b9b2949c1d857092250eff9888b5d7b1bc00e6
683a1a845f0c2d0f358d62a450f710f960190f2f
f740cb6c2bb9973fe5a4dc3ac609e36436e719eb
7466b3a81dad69b01df5d4b1233734bc0454ced8
6848d637c7caf0d0c8a7030dd45fca87cbbef339
f158dd1eea5a99f9a93d9acde8a57e04eb028bbb
21f5951d5347d2e728986a447e4bbafe1076f9bd
9199e664482d2277c8a61f491da3be703662502f
acb517dc5ec2376176cc3116bebfdf71d314663b
002b409fa931fb2cd154ba4affc1092de80a797d
f899824e38a6d260df9b79d72b40899617819113
2da7e0aea8f6392b2cc0858a3d0d0a67dd51e9b9
3d496563984c73e129577da8ca87d3e823fdcce4
704f1655ce9127d7aab6d82660b48a127b5f00cadd7282acb03c440f21dae5e2
8f8d01131ef7a66fd220dc91388e3c21988d975d54b6e69befd06ad7de9f6079
a86ed15ca8d1da51ca14e55d12b4965fb352b80e75d064df9413954f4e1be0a7

KPMG

KPMG Cyber Threat Intelligence Platform

Trigona- Emerging New Ransomware

Indicators of Compromise: Hashes
da32b322268455757a4ef22bdeb009c58eaca9717113f1597675c50e6a36960a
e97de28072dd10cde0e778604762aa26ebcb4cef505000d95b4fb95872ad741b
fa6f869798d289ee7b70d00a649145b01a93f425257c05394663ff48c7877b0d
fb128dbd4e945574a2795c2089340467fcf61bb3232cc0886df98d86ff328d1b
19667eba21a1caefda0a23cb43bdcb09070944e7cf7e3c2c11de1ba036677f09
09a5f38e6d534378583eb30ac6d893211983367cb0e01b58a11ef8933eb1f9a0
4724ee7274c31c8d418904ee7e600d92680a54fecdac28606b1d73a28ecb0b1e
e5cf252041045b037b9a358f5412ae004423ad23eac17f3b03ebef7c8147a3bb
5603d4035201a9e6d0e130c561bdb91f44d8f21192c8e2842def4649333757ab
c5d09435d428695ce41526b390c17557973ee9e7e1cf6ca451e5c0ae443470ca
248e7d2463bbfee6e3141b7e55fa87d73eba50a7daa25bed40a03ee82e93d7db
8cbe32f31befe7c4169f25614afd1778006e4bda6c6091531bc7b4ff4bf62376
efb688214c3fe5d9273ec03641cf17af5f546b11c97a965a49f8e617278ac700
f64211b0a49589bb53523dfb88eb9937ab88c8fcea98e2aabcbee90f1828e94e
11b0e9673bbeb978aa9b95bcad43eb21bbe0bbaaf7e5a0e20d48b93d60204406
eda603f4d469d017917f5d6affeb992fdf3b7971e49868ece8c38fb8e6f8b444
c4529a061f205aaee46c219123d15059d2161df2bd7c7b738dd2a2c1ffd8d3ee
170fa5d29cdb562d41a054abf2a57ca29fc233805b59692a1a57ebf25449be7c
197f4933680a611ad2234a22769bd079885f81956221ec0de172d5a19eab648e
1017fcf607a329bb6ad046181c3656b686906a0767fff2a4a3c6c569c2a70a85
761b78ddab55b4e561607ce5ce9d424a7aec4f1994aad988f0612b096cdd1d6d
097d8edb1762d7d3ded4360a9f5b4673a898937421f36853d2f5cde77e1bac93
4a06231957c53dee1a11ff3eb84caad082f18761aee49e72d79c7f1d32884e34
24123421dd5b78b79abca07bf2dac683e574bf9463046a1d6f84d1177c55f5e5
c7a930f1ca5670978aa6d323d16c03a97d897c77f5cff68185c8393830a6083f